

2012JUN30

ADDITION TO D5NR POLICY MANUAL, CHAPTER 2.

SAFEGUARDING PII

Q. Safeguarding/Protecting Personally Identifiable Information (PII).

1. Item 7 in the Commandant's Letter of Promulgation directs privacy compliance. Enrollment paperwork contains the most PII, however, other information such as patrol schedules and attendance of CG high ranking officers at a conference or meeting should be safeguarded. Also, medical information regarding injury reporting and communications may contain PII.
2. Enrollment Data. All enrollment forms must be held to the highest degree of protection. Copies of the ANSC-7001 shall **not** be made or maintained on file. The Unit leadership should already have contact information.
  - a. Incomplete enrollment forms shall be given to the applicant for safe keeping. Once the package is completed, the FC must immediately place the documents in a sealed envelope and mail directly to DIRAUX.
  - b. Enrollment packages that are physically brought to the DIRAUX office must be in a sealed envelope and marked accordingly, whether given directly to DIRAUX staff or put in the drop box after hours.
3. Operations.
  - a. Operational Security (OPSEC): Patrol schedules shall not be shared over the internet or via email between members. The DSO-OP and the ADSO-OPs are authorized to send Patrol Schedules to the [SecDelBayCC@uscg.mil](mailto:SecDelBayCC@uscg.mil) email in-box each Friday during the patrol season. Division SO-OPs are also authorized to report upcoming Patrol activity to the ADSOs for further reporting to the Sector. All members must avoid unnecessary forwarding or email sharing of patrol schedules and OPSEC information. Any information as to when, who, where, and why operations are conducted is to be handled carefully and not disclosed to the public. This type of sensitive operational information shall not be shared with anyone who does not have a need to know.
  - b. Communications Security (COMSEC): All Radio Communications must follow standard protocol and proper radio policies when in use. All members communicating on clear/open frequencies must be conscious of the type of information they are sharing over the radio and avoid passing any sensitive operational information that may be intercepted by our adversaries.

4. Faxed Submissions. Paperwork that is faxed to the DIRAUX office must not contain PII **unless** DIRAUX staff is notified prior to faxing.
5. Disposal of PII. All forms of PII must be shredded when the information is no longer required. Data containing an individual's PII must be given to the applicant or member for their own safekeeping or disposal at their discretion. No circumstance shall warrant anyone to hold onto another's PII.